PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-020117
(43)Date of publication of application : 28.01.1994

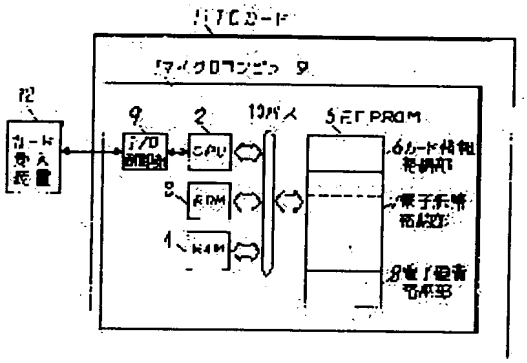
(51)Int.Cl. G06K 19/07

(21)Application number : 03-301663
(22)Date of filing : 18.11.1991

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TAKAGI SHINYA
MUTO YOSHIHIRO

(54) IC CARD

(57)Abstract:
PURPOSE: To provide an IC card to be used in a system moving electronized information (electronic note, for instance) between two persons while securing security and privacy simultaneously.
CONSTITUTION: The electronic note stored in an electronic note storage part 7 is protected with a CPU 2 and a unfair access can not be made for it from an outside. Further, when the electronic note is transmitted to other IC cards, it is safe since a proper ciphering processing can be performed by the CPU 2. The information on the possessor of an IC card 11 is not added to the electronic note at all and the note is circulated as a proper electronic note in a state that the only electronic signature of issuing origin of the electronic note is added.



LEGAL STATUS

[Date of request for examination]	05.03.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	withdrawal
[Date of final disposal for application]	10.01.1995
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It can have a processing control means, the nonvolatile memory for storing data, and an I/O means for transmitting and receiving said data between the exteriors at least, and the data stored in said nonvolatile memory can rewrite electrically. And the IC card which has further a field for storing the electronic bond with which the electronic signature read-out and the writing from the outside are possible, and according [said nonvolatile memory] to data issue-origin was added through said I/O means and said processing control means.
[Claim 2] The IC card according to claim 1 with which nonvolatile memory is characterized by having a field for storing the data with which the electronic signature by data issue-origin is not added.
[Claim 3] The IC card according to claim 1 characterized by having the operation part which calculates by using a private key for the electronic bond with which the electronic signature by data issue-origin was added, and the random number inputted from the outside.
[Claim 4] The IC card equipped with the nonvolatile memory which has a field for holding the information that a personal identification number is collating ending.
[Claim 5] The IC card which has a decision means to send the signal to which it judges whether the conditions as which the data read outside were determined are fulfilled, it restricts when filling, and the input of a personal identification number is urged.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Industrial Application] This invention relates to the IC card used by the system to which the information electronized [ticket / cash, the check, or] is moved among 2 persons.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] Electronic transfer of fund is used for inter-bank settlement of accounts etc. for the purpose of speeding up and the cost reduction of processing, and cashless payment-ization of a social system -- also in an individual life, the issue number of sheets of magnetic cards, such as an ATM card and a credit card, increases rapidly -- is progressing.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] According to this invention, the system which secures security and privacy to coincidence can be built as mentioned above by circulating the electronic bond which does not add any information about an IC card possessor using the IC card which has arithmetic proficiency.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] The bank etc. is the system by which migration of money data etc. is performed under management of a specific engine, and the present system has the problem of the privacy that an individual consumption trend etc. is altogether held by this specific engine.
[0004] It aims at offering the IC card used by the system to which the electronized information is moved among 2 persons, securing security without this invention's canceling the above-mentioned trouble and being managed by the specific engine.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] In order to solve this trouble the IC card of this invention It has a processing control means, the nonvolatile memory for storing data, and an I/O means for transmitting and receiving said data between the exteriors. The data stored in said nonvolatile memory are possible for read-out and the writing from the outside through said I/O means and said processing control means. And said nonvolatile memory considers as the configuration which has a field for storing the electronic bond with which the electronic signature by data issue-origin was added.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

OPERATION

[Function] The electronic bond stored in nonvolatile memory is protected by the processing control means by this configuration, and cannot be unjustly accessed from the outside by it. Furthermore, in case this electronic bond is transmitted to other IC cards, since suitable cipher processing can be performed by the processing control means, it is safe. Where no information about the possessor of an IC card was added to the electronic bond but only the electronic signature of electronic bond issue-origin is added on the other hand, it circulates as a just electronic bond. This is the same as circulation of current currency, and an IC card possessor's privacy is secured.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EXAMPLE

[Example] Hereafter, it explains, referring to a drawing about one example of this invention. First, as shown in drawing 2 , the electronic bill 21 treated by this example consists of amount-of-money information 22, a management number 23, and a digital signature 24. The engine which manages the issue business of the electronic bill 21 performs secret data processing to the amount-of-money information 22 and the management number 23, and only this issue engine can generate a digital signature 24. Moreover, if the management number 23 changes at least, the digital signature 24 to this will also change. That is, the electronic bill 21 cannot be forged or altered except a right issue engine. Moreover, if the electronic bill 21 should be reproduced by giving the consecutive number unique as a part of management number 23, it becomes possible to discover this.
[0008] Next, the IC card used by drawing 1 by this example is explained. Drawing 1 is the block diagram of the microcomputer 1 built in IC card 11 used by this example. A microcomputer 1 As ROM3 for storing CPU2 and the program which manage control of the whole microcomputer 1, and a working area at the time of program execution By I/O control section 9 for transmitting and receiving data between EEPROM5 for storing RAM4.used and the data written from card acceptance equipment 12, and card acceptance equipment 12, and bus 10 which connects ROM3, RAM4, and EEPROM5 with CPU4 It is constituted. CPU2 must be minded, in order to access the data stored in EEPROM5 from card acceptance equipment 12 so that I may be easily understood from drawing 1 . Therefore, unjust access can be forbidden by controlling CPU2 by the suitable program stored in ROM3. Moreover, since this microcomputer 1 can be constituted from one chip, it cannot carry out direct access of the address line or the data line of a bus 10. Furthermore, since the program stored in ROM3 is mask-ized, those who try injustice cannot change this program so that often [oneself]. Thus, the data stored in EEPROM5 is [a safe point] the big description of microcomputer built-in IC card 11 physically.
[0009] Another big description of IC card 11 is a calculation function by CPU2, and it enables this to perform various operations mentioned later, such as encryption processing, in the IC card 11 interior.
[0010] EEPROM5 is constituted by the electronic coin storing section 8 for storing the electronic bill storing section 7 for storing the card information storing section 6 for storing the information (cryptographic key etc.) used by internal processing of an IC card, and the electronic bill 21 of drawing 2 , and the money data of a small sum as shown in drawing 1 . Although the electronic bill storing section 7 is equivalent to the present sheaf-of-notes ON ** and the electronic coin storing section 8 is equivalent to a coin purse, such operation is concretely explained below using drawing 3 besides drawing 1 and drawing 2 .
[0011] Drawing 3 is an example of the processing flow of the price payment at the time of doing some shopping in a dealer using the IC card by this example. Each block is realized by the program stored in ROM3 of drawing 1 . The customer and the dealer possess IC card 11 of drawing 1 , and IC cards 31 and 32 of the same configuration, respectively, and in case it pays, they insert them in the card acceptance equipment 33 of a dealer. For this reason, card acceptance equipment 33 has two IC card insertion openings. Card acceptance equipment 33 has the display section (not shown) for in addition to this displaying the keypad section (not shown) metallurgy frame for inputting the amount of money etc. etc. After IC cards 31 and 32 of two sheets are inserted in card acceptance equipment 33, the salesclerk of a dealer inputs the amount of money of goods from the keypad of card acceptance equipment 33. This amount of money is displayed on the display of card acceptance equipment, and a customer can check the value of this amount of money. If the amount of money is inputted, the random-number generation

directions section 34 of card acceptance equipment 33 will issue [generating a random number to IC card 32 of a dealer, and] directions. The random-number generation section 35 of IC card 32 of a dealer generates a random number r in response to these directions, and transmits to a customer's IC card 31. The key generation section 36 of a customer's IC card 31 generates a cryptographic key ks from the received random number r and the secret key km stored in the card information storing section 6 of drawing 1 . Since this cryptographic key ks makes the random number r the parameter, it turns into a key of this throwing away that pays and is used only for processing. On the other hand, IC card 32 of a dealer also has the key generation section 44 and the private key km which perform the same operation as the key generation section 36, and generates the key ks of the same value as said ks.

[0012] In order to give explanation more concrete about the following processing flows, suppose that the inputted amount of money is 2300 yen. On the other hand, the electronic bill storing section 7 (drawing 1) of a customer's IC card 31 shall consist of two or more records, and the electronic bill 21 (drawing 2) equivalent to 1000 yen shall be stored in four records of them. Since one electronic bill is stored in one record, the electronic bill of a total of 4000 cyclotomies will be stored. Moreover, the change data of 700 yen shall be stored in the electronic coin storing section 8, and the customer will possess a total of 4700 yen.

[0013] The payment directions section 37 of card acceptance equipment 33 takes out directions of payment to a customer's IC card 31 by using 2300 yen as data. The fraction processing section 38 of a customer's IC card 31 treats as a fraction 300 yen smaller than 1000 yen which is the smallest unit of an electronic bill, since these 300 yen are 700 or less yen stored in the electronic coin storing section 8, it performs subtraction processing, considers as change data with the difference new 400 yen, and writes in the electronic coin storing section 8. The change data stored in the electronic coin storing section 8 are only amount-of-money information to which the management number 23 or digital signature 24 like the electronic bill 21 are not given. Therefore, this change data can add processing of addition and subtraction inside an IC card.

[0014] Next, the electronic bill elimination section 39 checks that 2000 yen which remains are 4000 or less yen stored in the electronic bill storing section 7, and it eliminates it from the electronic bill storing section 7 while it sends the electronic bill for two records stored in the electronic bill storing section 7 to the authentication child adjunct 40. Since the management number 23 and the digital signature 24 are given by the issue engine, in the electronic bill 21 stored in the electronic bill storing section 7, amount-of-money information cannot be subtracted and added within an IC card. Therefore, in case it pays, the electronic bill itself is eliminated from the electronic bill storing section 7, and in the case of a receipt, processing in which additional writing is performed for the electronic bill itself in the electronic bill storing section 7 is performed.

[0015] Next, the authentication child adjunct 40 enciphers the whole by the cryptographic key ks which added and mentioned above the authentication child who mentions later to the electronic bill for two records received from the electronic bill elimination section 39, and a 300 yen fractional data, and transmits to card acceptance equipment 33 at them. When the data on a communication link are altered, this processing is based on the method constituted so that it could detect having been altered by verifying an authentication child by the side which received encryption data, and has some well-known methods.

[0016] The payment directions section 41 of card acceptance equipment 33 will send this encryption data to IC card 32 of a dealer as it is with directions of payment, if said enciphered data are received from a customer's IC card 31. The authentication section 42 of IC card 32 of a dealer checks that the authentication child was inspected and there has been no alteration, after decoding the encryption data received using the key ks generated by the key generation section 44 mentioned above. Restricting, when it is checked that there had been no alteration, the addition processing section 43 adds the amount of money of a fractional data to the amount of money of the change data which carry out additional writing to the electronic bill storing section 7 of IC card 32 of a dealer, and are stored in the electronic coin storing section 8 in the electronic bill for two decoded records, and updates the change data of the electronic coin storing section 8. Above, price payment processing is completed.

[0017] In the above example, although the case where the value of the change data of the electronic coin storing section 8 was beyond a value of a fractional data was described in payment processing of a customer's IC card 31, when the value of the change data of the electronic coin storing section 8 is under a value of a fractional data, the following processings are performed. For example, for 2300 yen, when the

amount of money of the change data of the electronic coin storing section 8 is 100 yen, it treats as 2300= 3000-700, and the amount of money which the salesclerk inputted considers as the change data new 800 yen which added the 700 above-mentioned yen to the change data of 100 yen stored in the current electronic coin storing section 8, and stores in the electronic coin storing section 8. Furthermore, the electronic bill for three records stored in the electronic bill storing section 7 is eliminated, and the electronic bill for these three records and a -700 yen fractional data are sent to IC card 32 of a dealer. In IC card 32 of a dealer, 3 record addition writing is carried out at the electronic bill storing section 7, and 700 yen is subtracted from the electronic coin storing section 8.

[0018] Next, the safety of this example is explained. The private key km mentioned above is common to all IC cards so that a customer can do shopping even in what dealer and anyone can do an exchange of money data. However, since km is stored in the card information storing section 6 of drawing 1 , it can be prevented from knowing km by even the possessor of an IC card by controlling CPU2 by the suitable program stored in ROM3. The amount of money exchanged cannot be altered without a customer and a salesclerk being detected by the authentication section 42, since it is also impossible to compute ks if km is not known. Moreover, since the IC card is not generating the random number r inside even if the 3rd person intercepts the information transmitted to the authentication section 42 from the input directions section 41 and inputs it into his own IC card, the right ks is uncomputable. Therefore, verification of an authentication child cannot be passed and such a malfeasance is not materialized. The information outputted from the authentication child adjunct 40 is intercepted, and even if it tries to use this information for the opportunity of another shopping, it finishes with the same reason unsuccessful. That is, it is impossible for it to be effective as long as it pays and is alike, and for the exchange between a customer's IC card 31 and IC card 32 of a dealer to alter this information exchanged in the meantime, or to reuse it, and safety is secured.

[0019] It is a premise that the private key km is held secretly, and, as for this safety, updating periodically is desirable. Moreover, in this example, the very simple method which used the secret key cryptosystem is shown, and it has the description that high-speed processing is attained. It is good to use public key encryption on the other hand, in order to raise safety more. Moreover, safety can be further raised by preparing the authentication section which checks the justification of the digital signature 24 of the electronic bill 21 in an IC card.

[0020] In the old example, when an IC card is found or it is stolen, an IC card can be used also except a just possessor. This is the same as the case of current cash. a wallet will be locked if an IC card is used -- as -- a personal identification number -- using -- him -- the person of an except can be prevented from using an IC card However, also in case the IC card only containing the money data of a small sum is used, since it is troublesome, it is desirable [inputting a personal identification number] that the important point/needlessness of the input of a personal identification number can be freely changed for IC card possessor itself. An example for realizing this is shown in drawing 4 .

[0021] Drawing 4 shows the configuration of RAM4 and EEPROM5 in an IC card, has the collating flag 51 as well as drawing 1 in RAM4 besides the card information storing section 6, the electronic bill storing section 7, and the electronic coin storing section 8, and has the locking flag 52 in EEPROM5. Hereafter, referring to drawing 4 , when not set with the case where the locking flag 52 is set, it divides and explains.

[0022] When the locking flag 52 is set, whenever it uses this IC card, the input of a personal identification number is needed. That is, since the information on a flag is lost whenever a card is discharged, whenever it uses an IC card, the input of a personal identification number is needed [when an IC card receives a personal identification number collating command and collates correctly the personal identification number inputted by the IC card possessor, the flag of the collating flag attaching part 51 in RAM4 is set, and access to the electronic bill storing section 7 etc. is attained after that, but].

[0023] On the other hand, the locking flag 52 receives a device dependent command (here, it is described as a unlocking command) with an IC card, and is cleared by collating correctly the personal identification number inputted by the IC card possessor (unlocking). Since it is stored in EEPROM, this information is held even if an IC card is discharged. If it unlocks the locking flag 52, collating of a personal identification number is unnecessary irrespective of the condition of the collating flag 51. An IC card possessor performs this unlocking processing for example, using a personal terminal. In case the IC card which it unlocked is used in a dealer etc., it is not necessary to input a personal identification number. In order to need the input of a personal identification number again from the condition of having unlocked, a certain device

dependent command (here, it is described as a locking command) is used. An IC card will set the locking flag 52, if a locking command is received.

[0024] Moreover, a card possessor cannot lock and unlock if needed, but it can also program so that an IC card may judge the important point/needlessness of a personal identification number input automatically according to the size of the amount of money which invests money from an IC card. That is, when larger than the value which has the inputted amount of money in the program stored in ROM3 of drawing 1 , the input of a personal identification number is urged, and when conversely small, the decision section which judges the input of a personal identification number to be unnecessary is prepared. The value used as the criteria of this decision is made into the value stored in the electronic hardening storing section 8, and also it can consider various approaches, such as considering as the value set as the card information storing section 6 by the IC card possessor.

[0025] As mentioned above, although the processing flow of the price payment at the time of a customer doing some shopping in a dealer was explained, when a customer pays in in an IC card from a bank account, or also when a dealer pays a bank account from an IC card, the same method as drawing 3 can realize in order to prevent the alteration of the amount of money, and reuse of commo data. In this example, no information on a proper is added to a customer's IC card 31 at the money data stored in IC card 32 of a dealer. That is, since a bank cannot hold an individual consumption trend etc. from this money data, either, individual privacy is securable.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram of the microcomputer built in the IC card of the example of this invention
[Drawing 2] The configuration of the electronic bill of the example of this invention
[Drawing 3] The processing flow [example / of this invention] of price payment
[Drawing 4] The configuration of EEPROM and RAM of other examples of this invention
[Description of Notations]
1 Microcomputer
2 CPU
3 ROM
4 RAM
5 EEPROM
6 Card Information Storing Section
7 Electronic Bill Storing Section
8 Electronic Hardening Storing Section
9 I/O-Hardware-Control Section
10 Bus
11 IC Card
12 Card Acceptance Equipment

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－20117

(43)公開日　平成６年(1994)１月28日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｋ　19/07				
		8623－5L	Ｇ０６Ｋ　19/ 00	Ｎ

審査請求　有　　請求項の数５(全　６　頁)

(21)出願番号　特願平3－301663

(22)出願日　平成３年(1991)11月18日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　髙木　伸哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武藤　義弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内

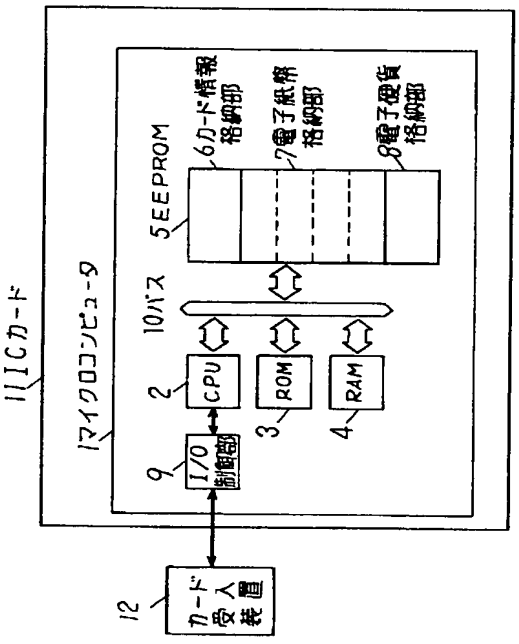
(74)代理人　弁理士　小鍛治　明　(外２名)

(54)【発明の名称】　ＩＣカード

(57)【要約】

【目的】　セキュリティとプライバシィを同時に確保しながら、電子化された情報（例えば電子紙幣）を２者間で移動させるシステムで用いられるＩＣカードを提供する。

【構成】　電子紙幣格納部７に格納された電子紙幣はＣＰＵ２により保護され、外部から不正にアクセスすることはできない。更にこの電子紙幣を他のＩＣカードに送信する際には、ＣＰＵ２により適切な暗号処理を施すことができるため安全である。一方、電子紙幣にはＩＣカード１１の所持者に関する情報は一切付加されず、電子紙幣の発行元の電子的な署名のみが付加された状態で正当な電子紙幣として流通する。



【特許請求の範囲】
【請求項１】少なくとも処理制御手段と、データを格納するための不揮発性メモリと、前記データを外部との間で送受信するための入出力手段とを備え、前記不揮発性メモリに格納されるデータが電気的に書き換え可能で、且つ前記入出力手段および前記処理制御手段を介してのみ外部からの読み出しおよび書き込みが可能であり、更に前記不揮発性メモリが、データの発行元による電子的な署名が付加された電子証書を格納するための領域を有するＩＣカード。
【請求項２】不揮発性メモリが、データの発行元による電子的な署名が付加されないデータを格納するための領域を有することを特徴とする請求項１記載のＩＣカード。
【請求項３】データの発行元による電子的な署名が付加された電子証書と、外部から入力された乱数とに秘密鍵を用いて演算を施す演算部を有することを特徴とする請求項１記載のＩＣカード。
【請求項４】暗証番号が照合済みであるという情報を保持するための領域を有する不揮発性メモリを備えたＩＣカード。
【請求項５】外部に読み出されるデータが定められた条件を満たすか否かを判断し、満たす場合に限り暗証番号の入力を促す信号を発信する判断手段を有するＩＣカード。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は現金、小切手あるいはチケット等の電子化された情報を２者間で移動させるシステムで使用されるＩＣカードに関する。
【０００２】
【従来の技術】処理の迅速化やコスト削減を目的として銀行間の決済等に電子資金移動が用いられ、個人生活においてもキャッシュカードやクレジットカード等の磁気カードの発行枚数が急増するなど社会システムのキャッシュレス化が進んでいる。
【０００３】
【発明が解決しようとする課題】現行のシステムは銀行等、特定の機関の管理下で金銭データ等の移動が行われるシステムになっており、個人の消費動向等がこの特定の機関によってすべて掌握されるというプライバシィの問題がある。
【０００４】本発明は上記の問題点を解消し、特定の機関に管理されることなく、かつセキュリティを確保しながら、電子化された情報を２者間で移動させるシステムで使用されるＩＣカードを提供することを目的とする。
【０００５】
【課題を解決するための手段】この問題点を解決するために本発明のＩＣカードは、処理制御手段と、データを格納するための不揮発性メモリと、前記データを外部との間で送受信するための入出力手段とを備え、前記不揮発性メモリに格納されるデータが前記入出力手段および前記処理制御手段を介してのみ外部からの読み出しおよび書き込みが可能であり、かつ前記不揮発性メモリが、データの発行元による電子的な署名が付加された電子証書を格納するための領域を有する構成としたものである。
【０００６】
【作用】この構成により、不揮発性メモリに格納された電子証書は処理制御手段により保護され、外部から不正にアクセスすることはできない。更にこの電子証書を他のＩＣカードに送信する際には、処理制御手段により適切な暗号処理を施すことができるため安全である。一方、電子証書にはＩＣカードの所持者に関する情報は一切付加されず、電子証書の発行元の電子的な署名のみが付加された状態で正当な電子証書として流通する。これは現在の通貨の流通と同じであり、ＩＣカード所持者のプライバシィが確保される。
【０００７】
【実施例】以下、本発明の一実施例について図面を参照しながら説明する。まず、図２に示すように、本実施例で扱われる電子紙幣２１は金額情報２２、管理番号２３およびデジタル署名２４から構成される。デジタル署名２４は、電子紙幣２１の発行業務を司る機関が金額情報２２と管理番号２３に対して秘密の演算処理を施したものであり、この発行機関のみが生成できる。また、少なくとも管理番号２３が変われば、これに対するデジタル署名２４も変化する。すなわち、正しい発行機関以外が電子紙幣２１を偽造または改ざんすることはできない。また、管理番号２３の一部としてユニークな連続番号を付与することにより、万一、電子紙幣２１が複製された場合、これを発見することが可能となる。
【０００８】次に図１により本実施例で使用されるＩＣカードについて説明する。図１は本実施例で使用されるＩＣカード１１に内蔵されるマイクロコンピュータ１のブロック図であり、マイクロコンピュータ１は、マイクロコンピュータ１の全体の制御を司るＣＰＵ２、プログラムを格納するためのＲＯＭ３、プログラム実行時の作業領域として使用されるＲＡＭ４、カード受入装置１２から読み書きされるデータを格納するためのＥＥＰＲＯＭ５、カード受入装置１２との間でデータの送受信を行うためのＩ／Ｏ制御部９、およびＣＰＵ４とＲＯＭ３、ＲＡＭ４、ＥＥＰＲＯＭ５を接続するバス１０により構成される。図１から容易に理解されるように、カード受入装置１２からＥＥＰＲＯＭ５内に格納されているデータをアクセスするためには必ずＣＰＵ２を介さなければならない。したがって、ＲＯＭ３に格納される適切なプログラムでＣＰＵ２を制御することにより、不当なアクセスを禁止することができる。また、このマイクロコンピュータ１は１チップで構成できるため、バス１０のア

ドレス線やデータ線を直接アクセスすることはできない。更に、ＲＯＭ３に格納されるプログラムはマスク化されているため、不正を試みる者がこのプログラムを自分に都合の良いように変更することはできない。このように、ＥＥＰＲＯＭ５内に格納されるデータが物理的に安全である点がマイクロコンピュータ内蔵型ＩＣカード１１の大きな特徴である。

【０００９】ＩＣカード１１のもう一つの大きな特徴はＣＰＵ２による演算機能であり、これにより、暗号化処理など後述する各種演算をＩＣカード１１内部で実行することが可能となる。

【００１０】図１に示すようにＥＥＰＲＯＭ５は、ＩＣカードの内部処理で使用される情報（暗号鍵等）を格納するためのカード情報格納部６、図２の電子紙幣２１を格納するための電子紙幣格納部７および少額の金銭データを格納するための電子硬貨格納部８により構成される。電子紙幣格納部７は現在の札束入れに相当し、電子硬貨格納部８は小銭入れに相当するが、これらの使用方法について、図１、図２の他、図３を用いて以下に具体的に説明する。

【００１１】図３は本実施例によるＩＣカードを用いて販売店で買い物をする際の代金支払いの処理フローの一例である。各ブロックは図１のＲＯＭ３に格納されるプログラムにより実現される。顧客および販売店はそれぞれ図１のＩＣカード１１と同じ構成のＩＣカード３１、３２を所持しており、支払いの際に販売店のカード受入装置３３にそれらを挿入する。このためにカード受入装置３３は二つのＩＣカード挿入口を有している。カード受入装置３３はこの他に、金額などを入力するためのキーパッド部（図示せず）や金額などを表示するためのディスプレイ部（図示せず）などを有している。２枚のＩＣカード３１、３２がカード受入装置３３に挿入された後、販売店の店員はカード受入装置３３のキーパッドから商品の金額を入力する。この金額はカード受入装置のディスプレイに表示され、顧客はこの金額の値を確認できる。金額が入力されるとカード受入装置３３の乱数生成指示部３４は販売店のＩＣカード３２に対して乱数を生成するよう指示を出す。販売店のＩＣカード３２の乱数生成部３５は、この指示を受けて乱数ｒを生成し、顧客のＩＣカード３１に送信する。顧客のＩＣカード３１の鍵生成部３６は受信した乱数ｒと、図１のカード情報格納部６に格納される秘密の鍵ｋｍとから暗号鍵ｋｓを生成する。この暗号鍵ｋｓは乱数ｒをパラメータとしているため、今回の支払い処理のためだけに使用される使い捨ての鍵となる。一方、販売店のＩＣカード３２も鍵生成部３６と同じ演算を実行する鍵生成部４４および秘密鍵ｋｍを有しており、前記ｋｓと同じ値の鍵ｋｓを生成する。

【００１２】以下の処理フローに関しては、説明をより具体的にするために、入力された金額が２３００円であるとする。一方、顧客のＩＣカード３１の電子紙幣格納部７（図１）は複数のレコードで構成されており、そのうちの４レコードに１０００円に相当する電子紙幣２１（図２）が格納されているものとする。１レコードに１つの電子紙幣が格納されるため、合計４０００円分の電子紙幣が格納されていることになる。また、電子硬貨格納部８には７００円という小銭データが格納されているものとし、顧客は合計４７００円を所持していることになる。

【００１３】カード受入装置３３の出金指示部３７は、２３００円をデータとして顧客のＩＣカード３１に出金の指示を出す。顧客のＩＣカード３１の端数処理部３８は、電子紙幣の最小単位である１０００円より小さい３００円を端数として扱い、この３００円が電子硬貨格納部８に格納されている７００円以下であるため減算処理を行い、差額の４００円を新しい小銭データとして電子硬貨格納部８に書き込む。電子硬貨格納部８に格納される小銭データは、電子紙幣２１のような管理番号２３やデジタル署名２４が付与されない金額情報のみである。したがって、この小銭データはＩＣカード内部で加減算の処理を加えることができる。

【００１４】次に電子紙幣消去部３９は、残る２０００円が電子紙幣格納部７に格納されている４０００円以下であることを確認し、電子紙幣格納部７に格納される２レコード分の電子紙幣を認証子付加部４０に送るとともに、電子紙幣格納部７から消去する。電子紙幣格納部７に格納される電子紙幣２１には、発行機関により管理番号２３やデジタル署名２４が付与されているため、ＩＣカード内で金額情報を加減算することはできない。したがって、支払いの際には電子紙幣そのものを電子紙幣格納部７から消去し、受取りの際には電子紙幣そのものを電子紙幣格納部７に追加書込みを行うといった処理を行う。

【００１５】次に認証子付加部４０は、電子紙幣消去部３９から受け取った２レコード分の電子紙幣と３００円の端数データに、後述する認証子を付加し、前述した暗号鍵ｋｓで全体を暗号化してカード受入装置３３に送信する。この処理は、通信上のデータが改ざんされた場合、暗号化データを受け取った側で認証子を検証することにより改ざんされたことを検出し得るよう構成された方式によるものであり、公知の方式がいくつかある。

【００１６】カード受入装置３３の入金指示部４１は、顧客のＩＣカード３１から前記暗号化されたデータを受け取ると、入金の指示とともに、この暗号化データをそのまま販売店のＩＣカード３２に送る。販売店のＩＣカード３２の認証部４２は、前述した鍵生成部４４により生成された鍵ｋｓを用いて受信した暗号化データを復号した後、認証子を検査して改ざんがなかったことを確認する。改ざんがなかったことが確認された場合に限り、加算処理部４３は、復号された２レコード分の電子紙幣

を販売店のＩＣカード３２の電子紙幣格納部７に追加書込みをし、電子硬貨格納部８に格納されている小銭データの金額に端数データの金額を加算して、電子硬貨格納部８の小銭データを更新する。以上で、代金支払い処理は完了する。

【００１７】以上の例では、顧客のＩＣカード３１の出金処理において、電子硬貨格納部８の小銭データの値が端数データの値以上である場合について述べたが、電子硬貨格納部８の小銭データの値が端数データの値未満である場合は以下のような処理を行う。例えば、店員が入力した金額が２３００円で、電子硬貨格納部８の小銭データの金額が１００円であった場合、２３００＝３０００－７００として扱い、現在電子硬貨格納部８に格納されている小銭データ１００円に上記７００円を加算した８００円を新たな小銭データとして電子硬貨格納部８に格納する。更に電子紙幣格納部７に格納される３レコード分の電子紙幣を消去し、この３レコード分の電子紙幣と－７００円の端数データとを販売店のＩＣカード３２に送る。販売店のＩＣカード３２では電子紙幣格納部７に３レコード追加書込みし、電子硬貨格納部８から７００円を減算する。

【００１８】次に本実施例の安全性について説明する。顧客がどこの販売店ででも買い物ができ、また、誰とでも金銭データのやり取りができるように、前述した秘密鍵ｋｍはすべてのＩＣカードに共通である。ところがｋｍは図１のカード情報格納部６に格納されているため、ＲＯＭ３に格納される適切なプログラムでＣＰＵ２を制御することにより、ＩＣカードの所持者でさえもｋｍを知ることができないようにすることが可能である。ｋｍがわからなければｋｓを算出することも不可能であるため、顧客および店員が認証部４２に検出されることなく、やり取りされる金額を改ざんすることはできない。また第３者が、入力指示部４１から認証部４２に送信される情報を盗聴して、それを自分のＩＣカードに入力したとしても、そのＩＣカードは内部に乱数ｒを生成していないため、正しいｋｓは算出できない。したがって、認証子の検証をパスすることはできず、このような不正行為は成立しない。認証子付加部４０から出力される情報を盗聴して、この情報を別の買い物の機会に使用することを試みたとしても、同じ理由で不成功に終わる。すなわち、顧客のＩＣカード３１と販売店のＩＣカード３２間のやり取りは、この支払いに限り有効であり、この間に交換される情報を改ざんしたり、再利用することは不可能であり、安全性が確保される。

【００１９】この安全性は、秘密鍵ｋｍが秘密に保持されていることが前提であり、定期的に更新することが望ましい。また、本実施例では秘密鍵暗号を用いた極めて簡易な方式を示しており、高速処理が可能となるという特徴を有している。一方、安全性をより向上させるためには公開鍵暗号を用いるのがよい。また、電子紙幣２１のデジタル署名２４の正当性を確認する認証部をＩＣカード内に設けることにより、更に安全性を向上させることができる。

【００２０】これまでの実施例では、ＩＣカードが拾得されたり盗まれた場合など、正当な所持者以外でもＩＣカードを使用することができる。これは現在の現金の場合と同じである。ＩＣカードを用いれば、財布に鍵を掛けるが如く、暗証番号を用いて本人以外の者がＩＣカードを使用できないようにすることができる。ただし、少額の金銭データしか入っていないＩＣカードを使用する際にも暗証番号を入力するのは煩わしいため、ＩＣカード所持者自身で自由に暗証番号の入力の要／不要を変更できることが望ましい。これを実現するための一例を図４に示す。

【００２１】図４はＩＣカード内のＲＡＭ４およびＥＥＰＲＯＭ５の構成を示すものであり、図１と同じくカード情報格納部６、電子紙幣格納部７、電子硬貨格納部８の他、ＲＡＭ４内に照合フラグ５１を有し、ＥＥＰＲＯＭ５内に施錠フラグ５２を有している。以下、図４を参照しながら、施錠フラグ５２がセットされている場合とセットされていない場合に分けて説明する。

【００２２】施錠フラグ５２がセットされている場合、このＩＣカードを使用する度に暗証番号の入力が必要となる。すなわち、ＩＣカードが暗証番号照合コマンドを受信し、ＩＣカード所持者により入力された暗証番号を正しく照合することにより、ＲＡＭ４内の照合フラグ保持部５１のフラグがセットされ、その後、電子紙幣格納部７へのアクセス等が可能となるが、カードが排出される度にフラグの情報は失われるため、ＩＣカードを使用する度に暗証番号の入力が必要となる。

【００２３】一方、施錠フラグ５２は、ＩＣカードがある専用コマンド（ここでは解錠コマンドと記す）を受信し、ＩＣカード所持者により入力された暗証番号を正しく照合することによりクリア（解錠）される。この情報はＥＥＰＲＯＭに格納されているため、ＩＣカードが排出されても保持される。施錠フラグ５２が解錠されていれば、照合フラグ５１の状態にかかわらず、暗証番号の照合は不要である。ＩＣカード所持者はこの解錠処理を例えば個人用端末を用いて行う。解錠されたＩＣカードを販売店等で使用する際、暗証番号を入力する必要はない。解錠された状態から再び暗証番号の入力を必要とするためには、ある専用コマンド（ここでは施錠コマンドと記す）を使用する。ＩＣカードは施錠コマンドを受信すると施錠フラグ５２をセットする。

【００２４】また、カード所持者が必要に応じて施錠および解錠するのではなく、ＩＣカードから出金する金額の大小に応じてＩＣカードが自動的に暗証番号入力の要／不要を判断するようにプログラミングすることもできる。すなわち、図１のＲＯＭ３に格納されるプログラム内に、入力された金額がある値より大きい場合は暗証番

号の入力を促し、逆に小さい場合は暗証番号の入力を不要と判断する判断部を設ける。この判断の基準となる値は、電子硬化格納部８に格納されている値とするほか、ＩＣカード所持者によりカード情報格納部６に設定される値とするなど、いろいろな方法が考えられる。

【００２５】以上、顧客が販売店にて買い物をした際の代金支払いの処理フローについて説明したが、顧客が銀行口座からＩＣカード内に入金する場合や、販売店がＩＣカードから銀行口座に入金する場合も、金額の改ざんや通信データの再利用を防ぐべく図３と同様の方式で実現できる。本実施例において、販売店のＩＣカード３２に格納される金銭データには顧客のＩＣカード３１に固有の情報は一切付加されていない。すなわち、銀行もこの金銭データから個人の消費動向等をつかむことができないため、個人のプライバシィを確保することができる。

【００２６】

【発明の効果】以上のように本発明によれば、ＩＣカード所持者に関する情報を一切付加しない電子証書を、演算能力を有するＩＣカードを用いて流通させることにより、セキュリティとプライバシィを同時に確保するシステムを構築することができる。

【図面の簡単な説明】

【図１】本発明の実施例のＩＣカードに内蔵されるマイクロコンピュータのブロック図

【図２】本発明の実施例の電子紙幣の構成

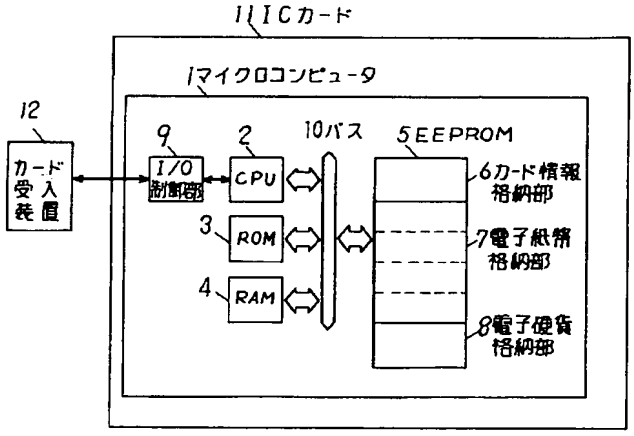
【図３】本発明の実施例の代金支払いの処理フロー

【図４】本発明の他の実施例のＥＥＰＲＯＭおよびＲＡＭの構成

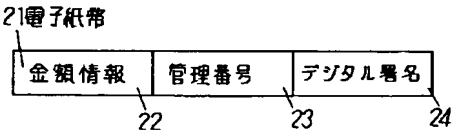
【符号の説明】

１　マイクロコンピュータ
２　ＣＰＵ
３　ＲＯＭ
４　ＲＡＭ
５　ＥＥＰＲＯＭ
６　カード情報格納部
７　電子紙幣格納部
８　電子硬化格納部
９　Ｉ／Ｏ制御部
１０　バス
１１　ＩＣカード
１２　カード受入装置

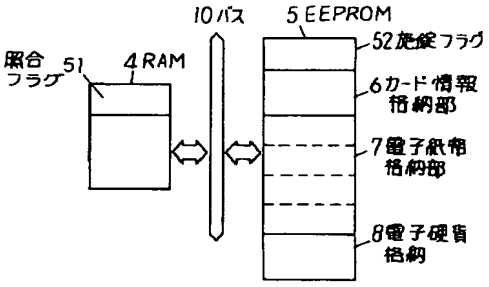
【図１】



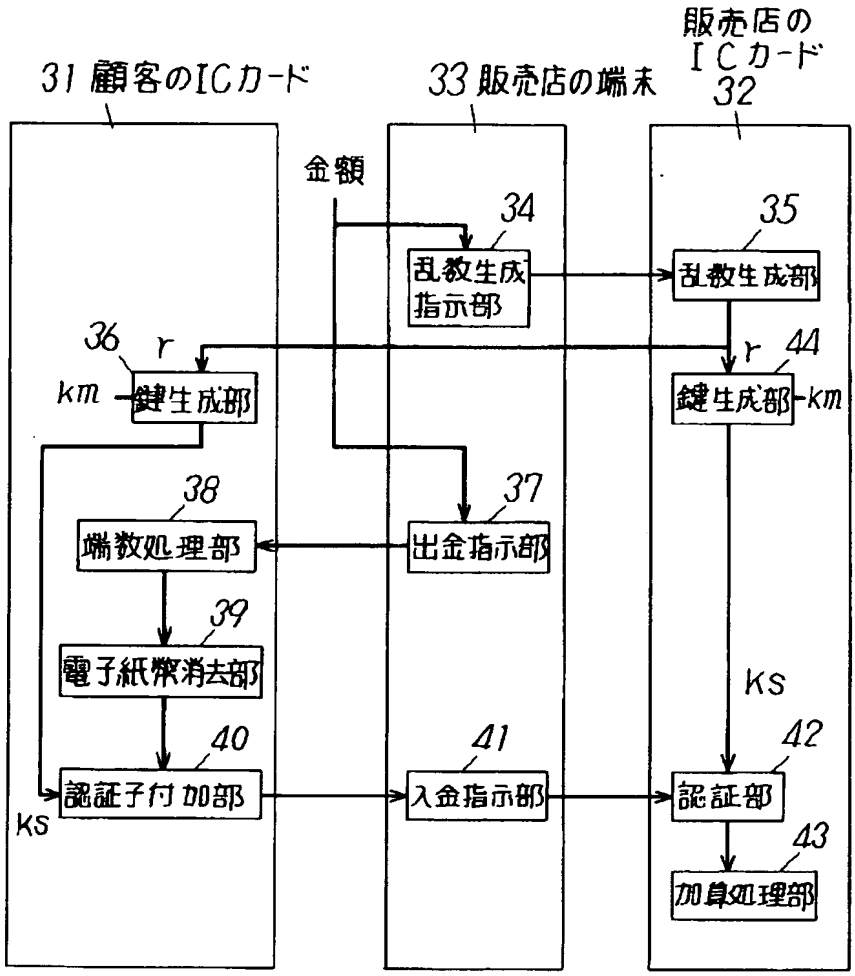
【図２】



【図４】



【図３】


販売店の
ＩＣカード
31 顧客のICカード
33 販売店の端末
32
金額
34
35
乱数生成
指示部
乱数生成部
36
r
r
44
km
鍵生成部
鍵生成部
km
38
37
端数処理部
出金指示部
39
電子紙幣消去部
KS
40
41
42
認証子付加部
入金指示部
認証部
KS
43
加算処理部